INFORMATION PAPER

SAIS-CB
1 February 2016

SUBJECT: New Army Training and Certification Tracking System (ATCTS) feature for the new DoD Directive 8140.01, DoD Cyberspace Workforce Framework (DCWF) initiative

1. Purpose. To provide an overview on the Cybersecurity workforce and management requirements for selecting DCWF work roles in ATCTS.

2. Background.

a. The DoD needs consistency when defining cyberspace work roles and qualifications to enable staffing for effective mission execution, particularly in joint environments. Therefore, the DoD Chief Information Officer led a working group of representatives from Department components to develop the DCWF. The DCWF is based on the integration of the National Initiative for Cybersecurity Education (NICE) workforce framework and the Joint Cyberspace Training and Certification Standards (JCT&CS), both of which reflect foundational contributions from the National Security Agency, to provide a lexicon of work roles by area of specialty, each with a baseline set of required knowledge, skills, and abilities (KSA) as well as functions.

b. The DCWF is a “living document”, reviewed annually and updated as necessary to reflect evolving DoD mission and workforce requirements.

c. The DoD Directive 8140.01 “ Cyberspace Workforce Management” and its corresponding manual DoD 8570.01-M “Information Assurance Workforce Improvement Program” do not reflect all of the work roles and qualifications needed to achieve the cyberspace mission. The DoD 8570.01-M addresses the only Information Assurance (IA) work roles. The DCWF stated above will identify the full spectrum of cyberspace workforce roles.

d. Additional issuances will be developed and reconciled with existing Information Technology/IA, Intelligence and Operations policies and directives, as needed to provide specific qualification and credentialing requirements for the work roles. These foundational tools will support DoD’s ability to collectively and strategically plan for the cyberspace workforce of the future.

e. Every person in a cyberspace work role has cybersecurity responsibilities. Position description criterion will include roles identified in the DoD Cyberspace Workforce Framework and the cybersecurity responsibilities within each role. Contract service requirements will also be updated to include cybersecurity responsibilities for all cyberspace work roles (technical, non-technical and leadership), For example, a system administrator would have a clear understanding of his or her responsibilities for hardening and maintaining

the integrity of systems, software, and networks; as well as for identifying suspicious cyber activity (anomaly detection), analysis and escalation.

f. The Privileged/Elevated Access to army Information Systems, Networks and Data was signed by LTG Ferrell on 1 February 2016. This memorandum establishes policy and responsibilities regarding privileged users. As part of the policy, Commands will continue to direct actions associated with the request for, receipt of and monitoring of Soldiers, civilians, contractors, vendors and any other individuals with privileged access to Army information systems, networks and data (i.e., users with elevated privileges, also known as privileged users).

3. Ongoing Actions.

a. In order to identify work roles for each Cybersecurity workforce person, an additional feature has been added to the Army Training and Certification Tracking System. This feature allows Cybersecurity personnel to add their DoD 8570.01-M category and level and their DoD Cyberspace Workforce role as noted in DoD Directive 8140.01.

b. This feature will continue to be updated for ease of usage in the system however the Army CIO/G6 Cybersecurity Training and Certification Team will need your recommendations to make it better.

4. Instructions: Below are the instructions for users and managers to reassess and override profiles to add specific DCWF roles within their profile.

a. Cybersecurity Workforce (reassessing profile). This process is the same for new registrations. You will be prompt to go through the questionnaire after logging on with access code.

(1) Users will need their account unverified by the ATCTS manager first before you can reassess your profile. Once it is unverified then the user can click on reassess and start the process.

(2) Click the answer that best describes your access to the IS for your primary duty position.

(3) Click on “Next Page” located at the bottom of page

(4) Choose the answer that best describes your position or title. This refers to the categories that we currently have under DoD 8570.01-M. You can only select one item.

(5) Choose the answer that best describes your management responsibilities (CE/NE/Enclave or do not manage other personnel). This question is only available if you choose “Manager” as your access to the IS.

(6) Choose the number of years you have worked in your current field.

(7) Choose your System Environment.

(8) Choose who you usually report to.

(9) Click Next page.

(10). The next page opens the area to choose the work role for their position in accordance with DoDD 8140.01 and the DoD Cyberspace Workforce Framework.

(11). The first set of options are the Categories (Securely Provision, Operate & Maintain, Oversight & Development, Protect & Defend, Analyze, Operate & Collect and Investigate) specified in the DCWF. Once the category is selected then the Specialty Area will show at the bottom of the page.

(12). Select one of the specialty areas.

(13). The specialty area will expand at the bottom with the work roles. Choose at least one by clicking on the "Add Role" link. Click the "More Info" link to show all the KSAs and Tasks associated with the work role, in a separate window or tab. You only have to close it to get rid of it. You can review the Tasks and KSAs before selecting the work role. You can select up to three work roles per position/duty.

(14). Select each additional role for your primary duty by selecting another Category or a different one depending on the work role you are performing.

(15). Once you are finished adding the work roles, if needed, you may drag and drop the work roles in order from top to bottom to put them in the correct order. Primary, Secondary and Third. Click "Next" to save your work role choices and continue.

(16). If you have an additional/embedded duty, then click the "I have an Additional/Embedded Duty" button; If you are finished adding your DCWF work roles then click on "I am Finished".

(17). Clicking "I have an Addition/Embedded Duty" takes you back through the same path of questions that you went through for your primary duty and work role(s).

b. **Managers Instructions for Overriding profiles in ATCTS:** Managers can override the DCWF position work roles and profile assignments

(1). Search for the individual's name.

(2). Click on "edit user".

(3). Click on override located to the right of the "Profile Assignment" and change the DoD 8570.01-M category and level.

(4). Choose the DoD 8570.01-M position. These will remain as long as DoD 8570.01-M is a valid issuance.

(5). Edit the work roles as necessary by click on the "edit roles" icon for the primary and secondary.

5. Please feel free to contact Doris Wright, 703-545-1703 or Liyla Yassin at 703-697-7610 for assistance. For additional information about NICE you can go to the website: https://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework